

PCT

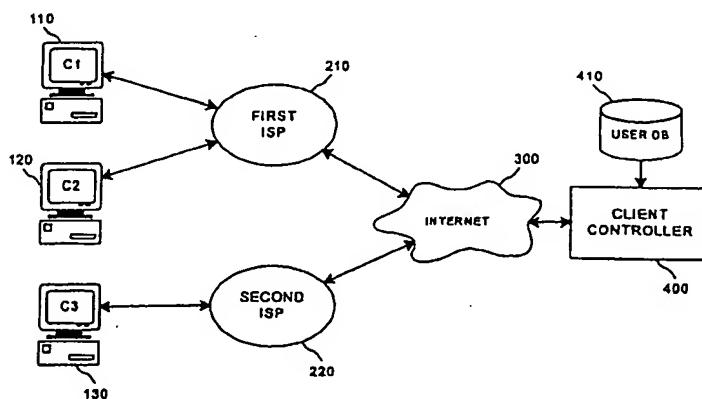
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ :	A1	(11) International Publication Number:	WO 99/53408
G06F 15/16, 17/30		(43) International Publication Date:	21 October 1999 (21.10.99)
(21) International Application Number:	PCT/US99/08058	(81) Designated States:	AU, CA, IL, IN, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) International Filing Date:	14 April 1999 (14.04.99)		
(30) Priority Data:	09/059,468 14 April 1998 (14.04.98) US	Published	<i>With international search report.</i>
(71) Applicant:	JUNO ONLINE SERVICES, INC. [US/US]; 120 West 45 Street, New York, NY 10036 (US).		
(72) Inventors:	DULAI, Dharmender, S.; 4th floor, 183 Broadway, New York, NY 10007 (US). MARUR, Vinod, R.; 89 West Lane #3, Ridgefield, CT 06877 (US). VITALE, Benjamin, F.; 223 E. 96 Street #5, New York, NY 10128 (US). ZENEL, Bruce, A.; Apartment 11D, 105 Lexington Avenue, New York, NY 10016 (US).		
(74) Agents:	ROSINI, James, E. et al.; Kenyon & Kenyon, Suite 700, 1500 K Street, Washington, DC 20005 (US).		

(54) Title: METHOD AND APPARATUS TO CONTROL A CLIENT IN A COMMUNICATIONS NETWORK



(57) Abstract

A method and apparatus to control a client (110) in a communications network (300) accessed by the client (110) through a service provider (210) independent of a client controller (400), such as an Internet service provider. When the client (110) starts the session, a start session message containing the user identity information is sent from the client (110) to the client controller (400) using the network (300) in accordance with a client control protocol. The client controller (400) can then determine whether the client (110) is authorized to use the network (300) based on the user identity information and, for example, a user database (410). If the client (110) is authorized, a session authorization message is sent to the client (110) authorizing the client (110) to use the network (300) for a predetermined period of time. When the client (110) stops accessing the network (300), the client (110) informs the client controller (400) by sending an end session message. If the client (110) wants to access the network beyond the predetermined period of time, the client (110) sends a continue session message to the client controller (400). If no end session or continue session message is received, the client controller (400) assumes that the client (110) is no longer accessing the network (300) at the end of the predetermined period of time. Other control messages, such as display and download commands, can also be sent from the client controller (400) to the client (110) using the client control protocol.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KC	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

METHOD AND APPARATUS TO CONTROL A CLIENT IN A COMMUNICATIONS NETWORK

FIELD OF THE INVENTION

5 The invention relates to communications networks. More particularly, the invention relates to a method and apparatus to control a client in a communications network.

BACKGROUND OF THE INVENTION

10

A packet-based communications network can transmit a data stream of bits in the form of packets of fixed or variable length for the purpose of moving information between computers. Each packet is routed through the network based on address information contained in the data stream. There are approximately 30 million users of packet networks in the U.S. The Internet, the largest and most well-known of the existing packet networks, connects millions of computers in countries across the world. In addition to the Internet, many companies use packet networks, locally or internally within the company, which are functionally modeled on the Internet. These packet networks, denoted "intranets" or "extranets," are compatible with the Internet Protocol (IP), a communications protocol for the address information of data packets transmitted using the Internet.

The World Wide Web, or "Web," represents a portion of the information on the Internet accessible through a graphical user interface software program, commonly known as a Web "browser." The Netscape NavigatorTM browser, available from Netscape Communications Corporation in Mountain View,

California, is one example of a Web browser. The Web is made up of "pages" that are stored and transmitted over the Internet using the Hyper Text Markup Language (HTML) by computer known as "servers." In general, a Web page can include combinations of text, graphics, sound, video and small application programs. A 5 Web page can also include a "link" which, when selected by a user, results in the automatic display of another Web page.

Typically, a user will access the Web by establishing a communications link with, or "logging onto," an Internet Service Provider (ISP), perhaps over a telephone line using a modem. When the user requests a Web page, the user's browser 10 communicates with the Internet through the ISP to retrieve the information related to the requested page. The ISP, which can serve thousands of users, generates revenue by charging each user a fee, such as a flat monthly fee, for the service. The ISP can also charge the user a time based fee in addition to, or instead of, the flat fee. Some ISPs also limit the amount of time that a given user can spend accessing the Internet.

15 The equipment required to operate an ISP can be very expensive, especially if the ISP expects to serve many users. The ISP may have to install, for example, a large number of phone lines, packet routers and communication switches. Moreover, the maintenance and technical support required to keep this equipment running can be difficult and expensive.

20 A company with the marketing ability required to attract a large number of users may not have the resources and expertise needed to provide Internet access. The company may, for example, be well known by users in a different, but related, field. Such company may also have, or not have, the resources and expertise needed to handle the billing and accounting functions typically provided by an ISP.

25 Conversely, a company with Internet access equipment may not be interested in, or be capable of, the marketing required to attract a large number of users. The company may also lack a support staff to answer user questions and an accounting system to track and bill users.

To solve this problem, it is known that a branded Internet access re-seller can 30 be established to handle the marketing and accounting aspects of Internet access.

Such a "virtual" ISP can lease Internet access time from a traditional "hardware capable" ISP, such as for a flat or time based fee. FIG. 1 is a block diagram of a known system of providing access to the Internet 300 through a virtual ISP 200. The virtual ISP 200 serves a number of users 110, 120, 130 by leasing access from a 5 number of ISPs 210, 220 that route communications to and from the Internet 300.

A user subscribes directly with the virtual ISP 200 for Internet access. The virtual ISP 200 assigns a user identifier (ID) and password to the user, and provides this information to one of the ISPs, such as the first ISP 210. The user is typically unaware of the identity of the ISP 210 that actually provides access to the Internet.

10 The virtual ISP 200 also provides the user with a client software program 114 to be used when accessing the Internet 300. As used herein, a "client" is a requesting computer program, and a "server" is a computer program that provides service to the client in response to the request.

To access the Internet 300, the user runs the client program 114 on a PC 110. 15 The client program 114 may include, for example, a communications software program and may be configured to display the name and logo of the virtual ISP 200. The client program 114 is configured to directly contact the ISP 210, using, for example, a modem 116. The client program 114 then presents the user's ID and password to the ISP 210 in order to "log onto" the system. Once the user logs onto 20 the ISP 210, the user can access the Internet 300 with a browser program 112. When the user is finished, he can "log off" the system to end the Internet access "session."

The virtual ISP 200 generally receives a periodic report from each ISP 210, 220 for billing purposes. For example, the ISP 210 may provide the virtual ISP 200 with a usage report each night listing the user ID of every user that accessed the 25 Internet 300 during the last 24 hour period. The report can also reflect the start time and end time, or length, of each such user session in order to determine how much the ISP 210 will bill the virtual ISP 200 for access. The report can also be used by the virtual ISP 200 to in turn bill each user directly.

One problem with known virtual ISP systems, however, is that the virtual 30 ISP 200 does not know which users are currently logged on. That is, although a

nightly report may be accurate for billing purposes, it does not reflect in real time which users are communicating with the Internet 300. A known protocol, called the Remote Authentication Dial In User Service (RADIUS) authentication protocol, can alert the virtual ISP 200 when a user logs on, but there is no way to inform the 5 virtual ISP 200 when the user logs off. A related protocol called, the RADIUS accounting protocol, can alert the virtual ISP 200 both when the user logs on and when the user logs off the system. However, the RADIUS accounting protocol operates between a virtual ISP 200 and a physical ISP 210, not between a virtual ISP 200 and a client program 114. Therefore, even the RADIUS accounting protocol 10 does not let the virtual ISP 200 exercise any control over the client program 114.

There are several reasons why a virtual ISP 200 may want to know which users are currently logged onto the system. For example, the virtual ISP 200 may want to communicate with all users who are currently on-line, such as to announce a special event. The virtual ISP 200 would not want to deal with a large number of 15 ISPs to determine which users are currently logged onto each ISP. The virtual ISP 200 may also be interested in which users are currently logged on for trouble shooting purposes.

Moreover, user fraud could be detected, and deterred, if the virtual ISP 200 could maintain an independent log of user access, instead of relying on the report 20 generated by the ISP 210. For example, a user that bypasses the client program 114 and contacts the ISP 210 directly would be detected by comparing the virtual ISP's log with the ISP's report. Similarly, such a log could be used to detect and resolve billing errors between the virtual ISP 200 and the ISP 210.

Another problem with known virtual ISP systems is that the virtual ISP 200 25 cannot directly control the client program 114 when a user is on-line. Suppose, for example, that the virtual ISP 200 wants to automatically install a new software release, or to update a list of access telephone numbers stored on the user's computer 110. Because the user PC 110 communicates with the ISP 210, and not with the virtual ISP 200, the virtual ISP 200 cannot instruct the client to download the new 30 information. Even if the virtual ISP 200 could arrange to have every individual ISP

perform such a download, this approach is cumbersome if the virtual ISP 200 leases access time from a large number of ISPs.

Similarly, the virtual ISP 200 may want to send a message to a user, such as a dialog window explaining why access to the network is being denied. Such an ability would reduce the number of customer support phone calls from users wondering if there is a technical problem with their connection. Because ISP 210 does not know the status of each user's account, and due to limitations in the RADIUS authentication protocol, the ISP 210 cannot perform this action. The virtual ISP 200 may also want to send a message warning a user that their monthly allotment of time is almost over, which is also not known by each ISP.

Another disadvantage of known virtual ISP arrangements is that real-time services cannot be offered to users. For example, the virtual ISP may want to offer users "chat rooms" that let users communicate with each other on a real-time basis. As part of this service, the virtual ISP might like to send a message to a user, letting the user know that certain other users are also currently logged on. Such a feature can typically be blocked by a user, if desired, for privacy reasons. Because the ISP 210 does not know if users are logged onto other ISPs, it cannot perform this service. Similarly, the virtual ISP does not know which users are currently logged on and cannot perform this service.

In view of the foregoing, it can be appreciated that a substantial need exists for a method and apparatus that provides a virtual ISP with real time information about, and control over, a client and solves the other problems, such as those associated with offering real-time services to a user, discussed above.

25 SUMMARY OF THE INVENTION

The disadvantages of the art are alleviated to a great extent by a method and apparatus to control a client via a client controller in a communications network, accessed by the client though a service provider independent of the client controller.

30 In one embodiment of the present invention, the client controller receives from the

client a start session message containing user identity information. The start session message is received using the communications network in accordance with a client control protocol. Based on the user identity information, the client controller can send to the client a control message using the communications network in
5 accordance with the client control protocol.

With these and other advantages and features of the invention that will become hereinafter apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a known system for providing Internet access through a virtual ISP.

5 FIG. 2 is a block diagram of a system that can be used to control a client according to an embodiment of the present invention.

FIGS. 3A to 3C are block diagrams of various client-initiated message exchanges according to embodiments of the present invention.

10 FIGS. 4A to 4C are block diagrams of various server-initiated message exchanges according to embodiments of the present invention.

FIG. 5 is a block flow diagram of a process for controlling a client according to an embodiment of the present invention.

DETAILED DESCRIPTION

15

The present invention is directed to a method and apparatus to control a client in a communications network. Referring now in detail to the drawings wherein like parts are designated by like reference numerals throughout, there is illustrated in FIG. 2 a block diagram of a system that can be used to control a client according to an embodiment of the present invention. Similar to those described in detail with respect to FIG. 1, a number of clients 110, 120, 130 access the Internet through physically different ISPs 210, 220 in a virtual ISP network.

According to an embodiment of the present invention, the virtual ISP can use an independent client controller 400 connected to the Internet 300 to provide real time information about, and to control, the clients 110, 120, 130. The client controller 400 is "independent" in the sense that it is physically separate from the ISPs 210, 220 that provide the clients 110, 120, 130 with access to the network over which the client controller 400 and clients 110, 120, 130 communicate, in this case the Internet 300. The client controller 400 includes a communications port for communicating using the Internet and a processor configured to execute commands

as described in detail below. In particular, the client controller 400 can be, for example, a group of server computers, or "server plant," capable of communicating with the clients 110, 120, 130 over the Internet 300. The server plant consists primarily of a series of servers dedicated to providing the services described (e.g., 5 authentication, control, etc.) to the clients. Specifically, these servers can be, for example, Sun Microsystems Sparc SS-20s and Sparc Ultra 2300s, running the Solaris operating system.

The client program installed on a user's PC, such as the client 110, displays, if desired, the name and logo of the virtual ISP. To initiate a communications 10 session, the user first logs onto the client application 110 by providing a user ID and password. The client 110 then directly dials the ISP 210 and provides the ISP with this user ID and password. The ISP 210 compares the user ID and password with authorization information that has been supplied by the virtual ISP, such as a list of authorized users. Alternatively, the ISP 210 contacts the virtual ISP 200 to authorize 15 the user using a protocol such as the RADIUS authentication protocol. After logging on with this first tier of direct authentication, the client 110 is configured to automatically send a message to the client controller 400 over the Internet 300.

The client 110 and client controller 400 communicate using a Client Control Protocol (CCP), which is a suite of special messages sent over the Internet 300 using 20 Transmission Control Protocol (TCP) packets having an appropriate IP address and TCP port number. Every TCP connection between a client and a server is defined by two pairs of information: the IP address and TCP port of the client and the IP address and TCP port of the server. The concept of multiple "ports" lets several applications share the same IP address. For example, the client 110 and client 25 controller 400 will each be assigned a unique IP address in the communications network, or Internet 300. The browser 112 will use one TCP port number, such as 80, to send and receive information, such as HTML information, over the Internet 300. The client program 114 will use a different TCP port number, such as 8505, to send and receive CCP messages.

30 In other words, CCP is an in-band signaling protocol that operates in parallel

with applications such as the browser 112 over the Internet 300. The CCP messages can be encrypted using known encryption techniques, if desired. As will be explained in detail with respect to FIGS. 3A to 3C and 4A to 4C, the client controller 400 uses the CCP to obtain information about the client 110, such as a start time and 5 an end time of the client's access to the communications network 300. Moreover, the client controller 400 can control the client 110 using the CCP, such as by authorizing access or commanding the client 110 to perform certain tasks.

Using CCP, the client 110 transmits to the client controller 400 a start session message, including user identity information such as the user ID and the IP 10 address of the client 110. This is used to allow the client controller 400 to perform a second tier of authentication and lets the controller 400 know that the client 110 is currently logged on. For example, the client controller 400 can match the user ID in the start session message with information in a user database 410. In addition to the user ID, the user database 410 can contain the user name, billing history and profile 15 information. If the user ID is not authenticated, the client controller 400 can command the client 110 to terminate the session with an appropriate CCP message.

If the user ID is authorized, the client controller 400 records the user ID and the time of day in a usage log. The usage log can be, for example, a database maintained by the client controller 400. When the client logs off of the ISP 210, the 20 client 110 uses CCP to inform the client controller 400 that the session has ended. This information can also be recorded in the usage log. In this way, the client controller 400 can determine which users are currently logged onto the system. This information can, for example, let a virtual ISP send a message to a user saying that certain other users are also currently logged on, allowing users to meet in real-time 25 chat rooms.

Some uses for CCP will now be described with respect to FIGS. 3A to 3C, which are block diagrams of various client-initiated message exchanges using CCP according to embodiments of the present invention. FIG. 3A shows the CCP start session message being sent from a client 100 to the client controller 400. If the 30 client controller 400 determines that the client 100 is not authorized, the session can

be denied with an appropriate CCP response. Denial of authorization could occur, for example, because the user has not paid the required fee. In such a case, the client software program 100 will automatically halt access to the Internet.

If the client is authorized, the client controller 400 can send a CCP session authorization message to the client 100 authorizing access to the Internet for a predetermined period of time, such as "n" minutes. For example, the client controller 400 may inform the client 100 that access to the Internet has been authorized for the next 30 minutes. In this case, the client controller 400 records the user ID and time of day in the usage log.

If the client 100 is still accessing the Internet, a CCP continue session request is automatically sent to the client controller 400, as shown in FIG. 3B, before the predetermined period of time expires. For example, the client 100 can be configured to automatically send a continue session request 25 minutes after being authorized to access the Internet for 30 minutes. At this time, if the client controller 400 determines that the client 100 is no longer authorized, the session continuation can be denied. This could be, for example, because the user has reached a monthly maximum allotment of time. Otherwise, the client controller 400 can send a CCP continuation authorization message telling the client 100 that access to the Internet has been authorized, by way of example, for another 30 minutes.

When the user logs off of the ISP, the client 100 sends a CCP end session message to the client controller 400 as shown in FIG. 3C. In this case, the client controller 400 records the user ID and time of day in the usage log. If the predetermined period of time expires and the client 100 has not sent either a continue session request or an end session message, the client controller 400 assumes that the session has been terminated and records the user ID and time of day in the usage log. By authorizing access for limited periods of time, the client controller 400 can infer that a session was terminated, for example, because the user's computer malfunctioned or its communication link, such as a telephone connection, was broken prematurely.

In this way, use of CCP enables monitoring by the client controller 400 of

which users are currently accessing the Internet. Based on the current usage log, the client controller 400 can determine in real-time all users that are logged onto the system at that moment and provide a real-time list of such users. Moreover, the virtual ISP can compare the end of day usage log with billing records from each ISP

5 to determine if users are accessing the Internet without using the client software. For example, if a user appears on an ISP billing record, but not on the virtual ISP's usage log, the user must be accessing the ISP without using the client software because no start session message was received by the client controller 400. The end of day usage log can also be used to audit and detect errors in an ISP's billing record, thus

10 saving the virtual ISP money.

In addition to client-initiated exchanges, FIGS. 4A to 4C illustrate various server-initiated CCP message exchanges according to embodiments of the present invention. As shown in FIG. 4A, the client controller 400 can send a display command to the client 100. The command can instruct the client to display, for example, a window containing a short message. In this way, when a user is denied access for any reason the client controller 400 can send an explanation to the user. Another example is a message to inform the user that they have newly arrived e-mail.

15

The client controller 400 can also send a download command to the client 20 100, as shown in FIG. 4B. This lets the client controller 400 automatically provide information to a user, such as a new software program, patch or a list of ISP phone numbers. Finally, as shown in FIG. 4C, the client controller 400 can send a terminate session command to the client 100. With any of these server-initiated commands, the client 100 can be configured to confirm, by sending a response to the 25 client controller 400, that the CCP command from the client controller 400 has been received or successfully completed.

FIG. 5 is a block flow diagram of a process that provides control of a client according to an embodiment of the present invention. After beginning at step 500, the client controller, such as the one shown in FIG. 2, receives a start session 30 message from a client, including the client's user ID, at step 510. If the client

controller determines that the client is not authorized to use the network at step 520, access is denied and a message is sent to the client explaining the denial at step 525.

If the client controller determines that the client is authorized at step 520, the user ID and time of day are recorded in the usage log at step 530. An authorization 5 message is then sent to the client to authorize the session for n minutes at step 540. If an end session message is received from the client at step 550, the user ID and time of day are recorded in the usage log at step 555 before the process ends at step 590. Similarly, if a continuation message is not received before the end of n minutes, the user ID and time of day are recorded in the usage log at steps 560 and 10 580.

If a continuation message is received at step 560, the client controller determines if continued access is authorized at step 570. If continued access is authorized, another authorization is sent and the process repeats beginning at step 540. If continued access is not authorized, access is denied and a message is sent to 15 the client explaining the denial at step 575. If desired, the denial can also be recorded into the usage log, although this step is not shown in FIG. 5.

As is known in the art, the methods described above can be performed by hardware, software, or some combination of software and hardware. When performed by software, the methods may be executed by a processor, such as a 20 general purpose computer, based on instructions stored on a computer-readable medium. Examples of a medium that store instructions adapted to be executed by a processor include a hard disk, a floppy disk, a Compact Disk Read Only Memory (CD-ROM), flash memory, and any other device that can store digital information. If desired, the instructions can be stored on the medium in a compressed and/or 25 encrypted format. As used herein, the phrase "adapted to be executed by a processor" is meant to encompass instructions stored in a compressed and/or encrypted format, as well as instructions that have to be compiled or installed by an installer before being executed by the processor.

Although various embodiments are specifically illustrated and described 30 herein, it will be appreciated that modifications and variations of the present

invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention. For example, although particular CCP message exchanges have been used to illustrate the present invention, it can be appreciated that other messages and
5 commands will also fall within the scope of the invention.

What is claimed is:

1. A method using a client controller to control a client in a communications network, the client accessing the communications network through a service provider independent of the client controller, comprising the steps of:
 - receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol; and
 - sending to the client a control message, the control message being sent from the client controller using the communications network in accordance with the client control protocol.
2. The method of claim 1, wherein said step of sending controls the client's access to the communications network.
- 15 3. The method of claim 2, wherein the control message is a session authorization message authorizing the client to use the communications network for a predetermined period of time.
- 20 4. The method of claim 3, further comprising the step of:
 - determining if the client is authorized to use the communications network based on the user identity information,
 - and wherein said step of sending a session authorization message is only performed if the client is authorized to use the communications network.
- 25 5. The method of claim 2, further comprising the step of:
 - determining if the client is authorized to use the communications network based on the user identity information,
 - and wherein the control message is a deny session message if the client is not authorized to use the communications network.

6. The method of claim 1, wherein the control message instructs the client to display a message to a user.
7. The method of claim 1, wherein the control message instructs the client to receive data.
8. The method of claim 1, further comprising the steps of:
recording information about a client session in a communications network usage log.

10

9. The method of claim 8, wherein the recorded information includes information associated with the user identity information and information associated with the time that the client session started.

15

10. The method of claim 3, further comprising the steps of:
receiving from the client a session continuation message containing the user identity information; and
sending to the client a continuation authorization message, based on the user identity information, authorizing the client to use the communications network for

20

- an additional predetermined period of time.

11. The method of claim 10, wherein the continuation authorization message is an additional session authorization message.

25

12. The method of claim 10, further comprising the step of determining if the client is authorized to continue to use the communications network based on the user identity information, and wherein said step of sending a continuation authorization message is only performed if the client is authorized to continue using the communications network.

13. The method of claim 8, further comprising the steps of:
receiving from the client an end session message containing the user identity
information; and
recording information about the end of the client session in the usage log.

5

14. The method of claim 8, further comprising the step of:
recording information about an end of the client session in the usage log if no
session continuation message has been received from the client during the
predetermined period of time.

10

15. The method of claim 8, further comprising the steps of:
receiving from the service provider a communications network usage report;
and
comparing the communications network usage report with the
communications network usage log to determine discrepancies.

16. The method of claim 1, further comprising the steps of:

sending to the client a session termination message instructing the client to
end the client session; and

recording information about the end of the client session in a usage log.

17. The method of claim 1, wherein the communications network is a packet
network.

25 18. The method of claim 17, wherein the packet network is the Internet and
the client control protocol is an in-band protocol transmitted using transmission
control protocol/Internet protocol.

19. The method of claim 1, wherein said step of determining is also based on
30 information stored in a user database.

20. A method using a client controller to monitor a client in a communications network, the client accessing the communications network through a service provider independent of the client controller, comprising the steps of:

5 receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communication network in accordance with a client control protocol; and recording in a communications network usage log information associated with the user identity information and information associated with the time that the
10 start session message was received.

21. The method of claim 20, wherein the communications network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.

15

22. A client controller to control a client in a communications network, the client accessing the communications network through a service provider independent of the client controller, comprising:

a communications port capable of receiving from the client a start session
20 message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol;

a user database containing information associated with the user identity information; and
25 a client control processor coupled to said communications port and said user database, said client control processor being configured to send a control message to the client, the control message being sent from the client controller using the communications network in accordance with the client control protocol.

30 23. The client controller of claim 22, wherein the control message controls

the client's access to the communications network.

24. The client controller of claim 23, wherein the control message is a session authorization message authorizing the client to use the communications
5 network for a predetermined period of time.

25. The client controller of claim 22, wherein the control message instructs the client to display a message to a user.

10 26. The client controller of claim 22, wherein the control message instructs the client to receive data.

27. The client controller of claim 22, said client control processor being further configured to record information about a client session in a communications
15 network usage log.

28. The client controller of claim 22, wherein the communications network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.

20

29. An apparatus to control a client in a communications network, the client accessing the communications network through a service provider independent of a client controller, comprising:

means for receiving from the client a start session message containing user
25 identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol;

means for determining if the client is authorized to access the communications network; and

means for sending to the client a session authorization message, the session
30 authorization message being sent from the client controller using the

communications network in accordance with the client control protocol.

30. The apparatus of claim 29, wherein the control message controls the client's access to the communications network.

5

31. The apparatus of claim 29, wherein the control message is a session authorization message authorizing the client to use the communications network for a predetermined period of time.

10 32. The apparatus of claim 29, wherein the communications network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.

15 33. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to control a client's access to a communications network, the client accessing the communications network through a service provider independent of a client controller, said steps comprising:

20 receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol; and sending to the client a control message, the control message being sent from the client controller using the communications network in accordance with the client
25 control protocol.

34. The article of manufacture of claim 33, wherein said step of sending controls the client's access to the communications network.

30 35. The article of manufacture of claim 33, wherein the control message is a

session authorization message authorizing the client to use the communications network for a predetermined period of time.

36. The article of manufacture of claim 33, wherein the control message
5 instructs the client to display a message to a user.

37. The article of manufacture of claim 33, wherein the control message
instructs the client to receive data.

10 38. The article of manufacture of claim 33, further comprising the steps of:
recording information about a client session in a communications network
usage log.

15 39. The article of manufacture of claim 33, wherein the communications
network is the Internet and the client control protocol is an in-band protocol
transmitted using transmission control protocol/Internet protocol.

40. A method of using a communications network having a client controller,
comprising the steps of:
20 accessing the communications network through a service provider
independent of the client controller;
sending to the client controller a start session message containing user
identity information; and
receiving from the client controller a control message, the control message
25 being received by the client using the communications network in accordance with a
client control protocol.

41. The method of claim 40, wherein the control message is a session
authorization message authorizing the client to use the communications network for
30 a predetermined period of time.

42. The method of claim 40, wherein the control message instructs the client to display a message to a user.

5 43. The method of claim 40, wherein the control message instructs the client to receive data.

10 44. The method of claim 40, wherein said step of accessing comprises complying with a first authentication procedure performed by the service provider and said step of sending comprises complying with a second authentication procedure performed by the client controller, the second authentication procedure being independent of the first authentication procedure.

15 45. The method of claim 40, further comprising the step of:
sending a session continuation message to the client controller prior to the end of the predetermined period of time.

46. The method of claim 40, further comprising the step of:
sending an end session message to the client controller.

20 47. The method of claim 40, wherein the communications network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.

25 48. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to use a communications network having a client controller, said steps comprising:
accessing the communications network through a service provider
30 independent of the client controller;

sending to the client controller a start session message containing user identity information; and

receiving from the client controller a control message, the control message being received by the client using the communications network in accordance with a
5 client control protocol.

49. The article of manufacture of claim 48, wherein the control message is a session authorization message authorizing the client to use the communications network for a predetermined period of time.

10

50. The article of manufacture of claim 48, wherein the control message instructs the client to display a message to a user.

15

51. The article of manufacture of claim 48, wherein the control message instructs the client to receive data.

20

52. The article of manufacture of claim 48, wherein said step of accessing comprises complying with a first authentication procedure performed by the service provider and said step of sending comprises complying with a second authentication procedure performed by the client controller, the second authentication procedure being independent of the first authentication procedure.

25

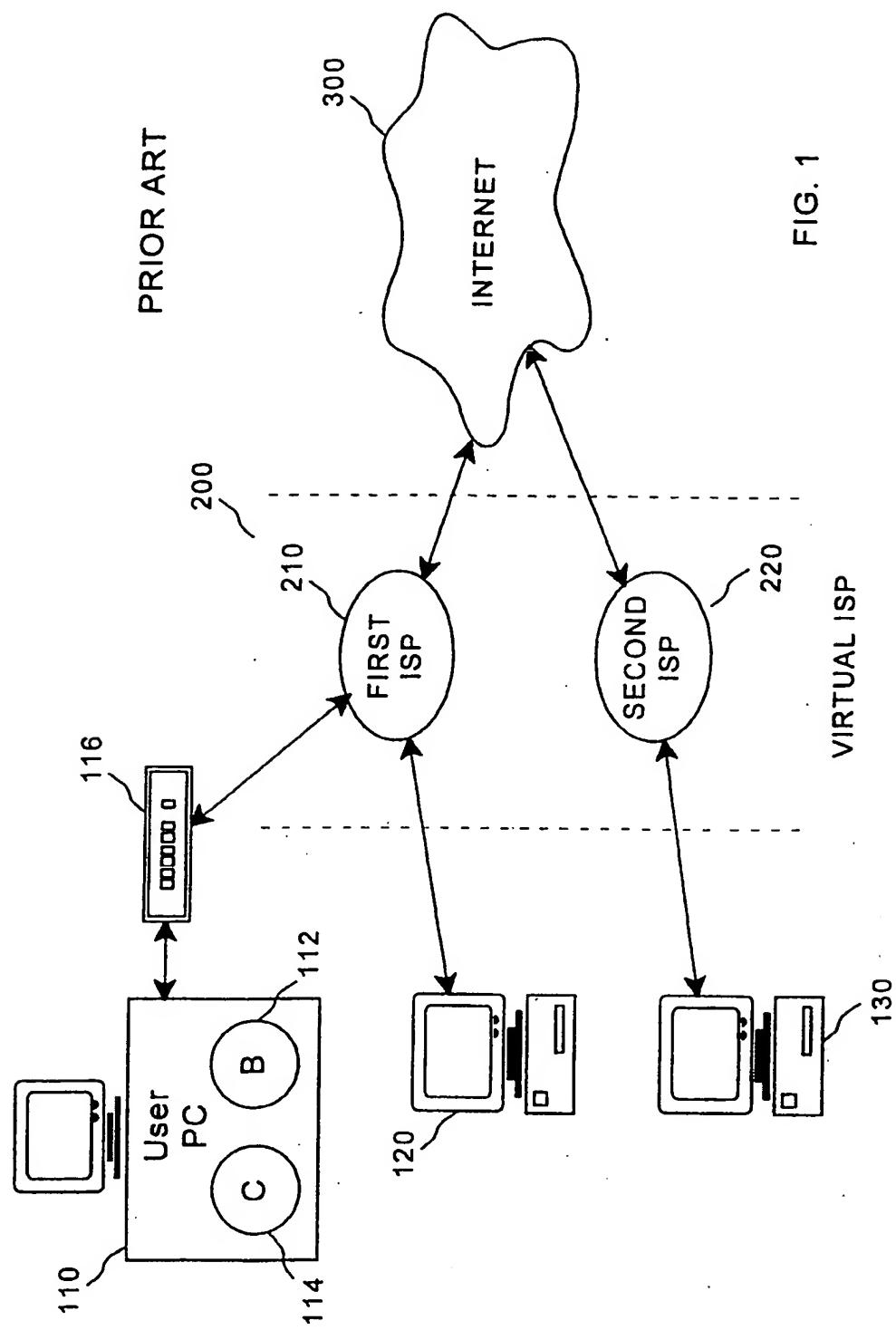
53. The article of manufacture of claim 48, further comprising the step of: sending a session continuation message to the client controller prior to the end of the predetermined period of time.

30

54. The article of manufacture of claim 48, further comprising the step of: sending an end session message to the client controller.

55. The article of manufacture of claim 48, wherein the communications

network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.



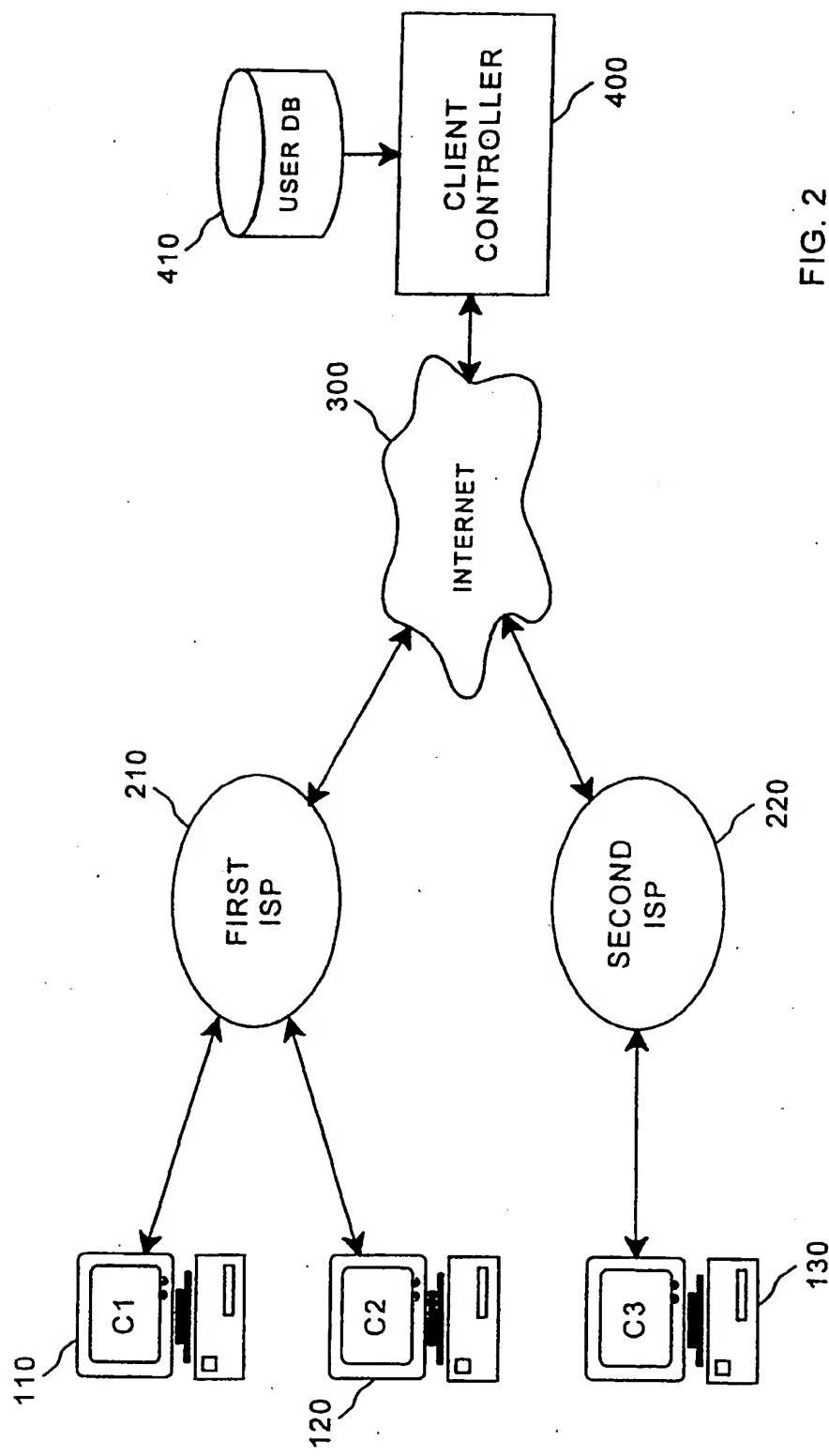


FIG. 2

FIG. 3(A)

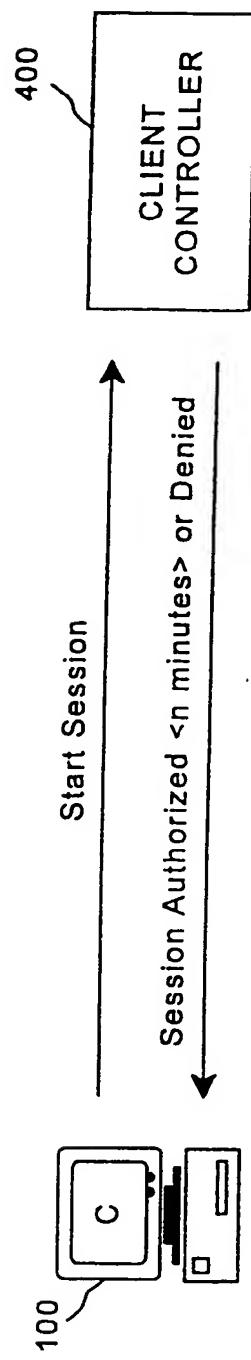


FIG. 3(B)

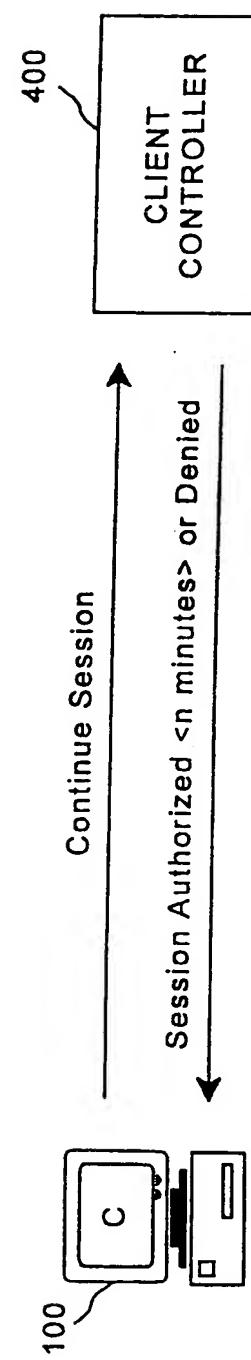


FIG. 3(C)

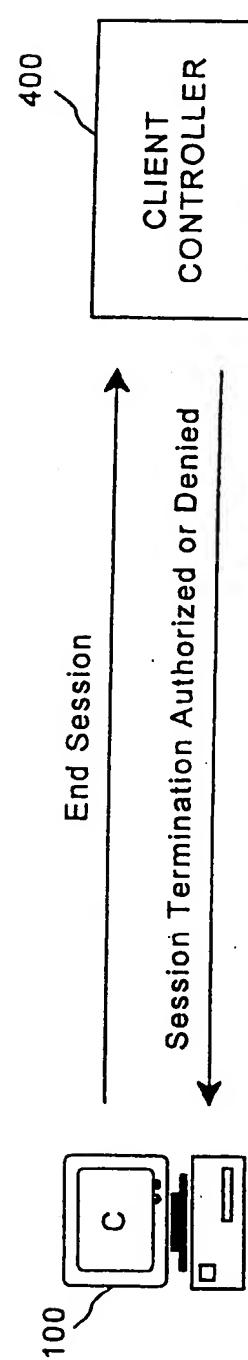


FIG. 4(A)

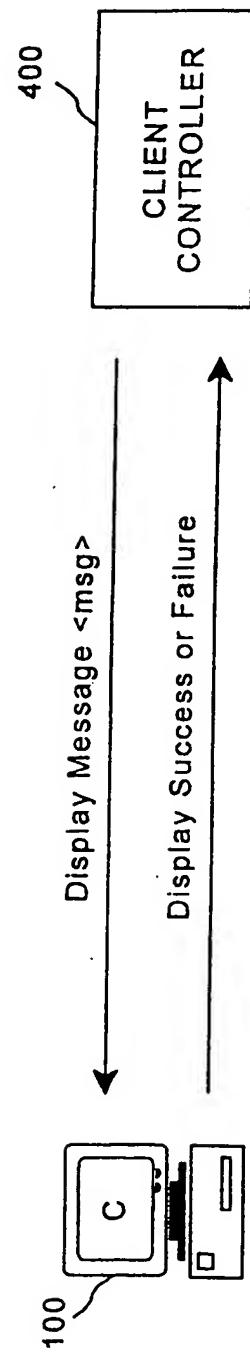
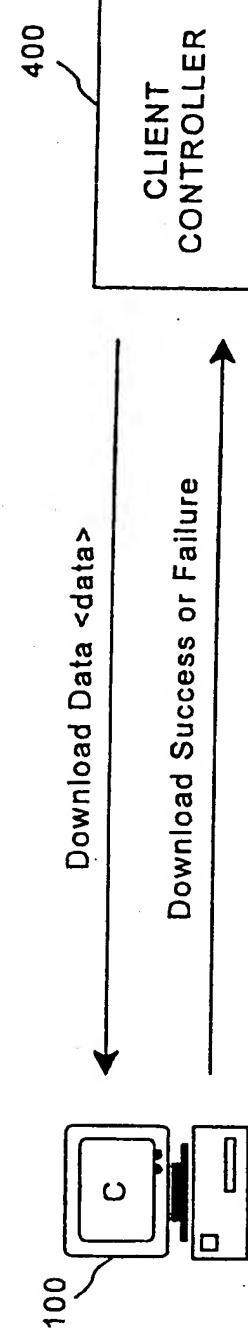
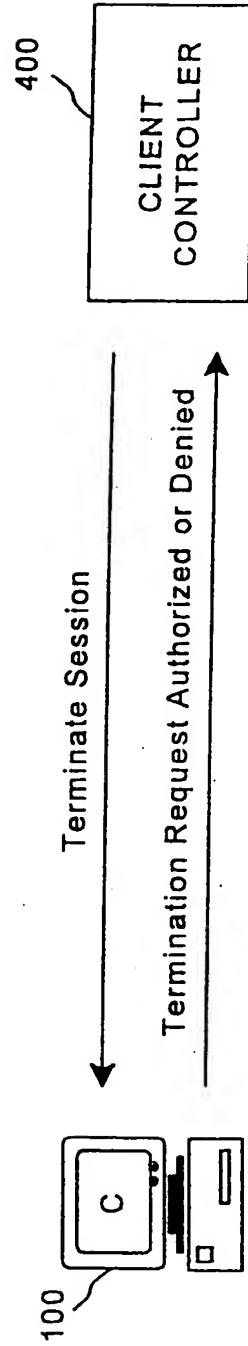
FIG. 4(B)
4/5

FIG. 4(C)



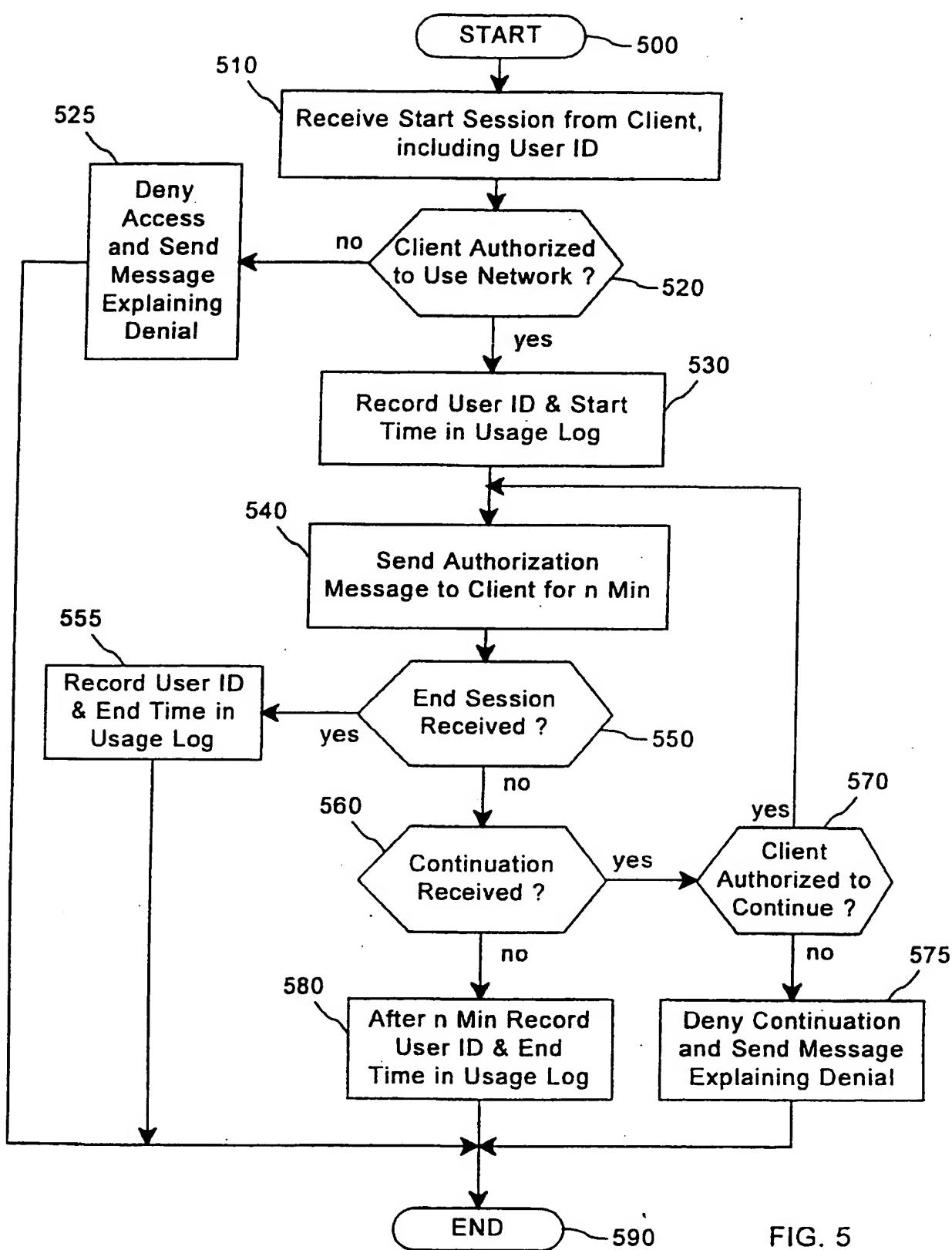


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/08058

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 15/16, 17/30
US CL : 709/225, 229, 203; 707/104

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U S 709/203, 217, 218, 219, 223, 224, 225, 229,; 707/10, 104

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Elsevier Science Server (Non Patent Literature), APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,708,780 A (LEVERGOOD et al.) 13 January 1998, fig. 2B, cols. 5-8, especially col. 5 lines 3-16, col. 5 lines 42-65, col. 6 lines 5-16, col. 6 line 58 to col. 7 line 20, col. 8 lines 14-58.	1-9, 15-43, 47-51, 55
Y		-----
Y, P	US 5,796,393 A (MACNAUGHTON et al.) 18 August 1998, cols. 6, 8, 11, 16, col. 15 lines 1-3.	10-14, 44-46, 52-54
A	US 5,481,720 A (LOUCKS et al.) 02 January 1996.	1-55
A	US 5,889,958 A (WILLENS et al.) 30 March 1999.	1-55

Further documents are listed in the continuation of Box C. See patent family annex.

Special categories of cited documents	*T*	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
document defining the general state of the art which is not considered to be of particular relevance	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
earlier document published on or after the international filing date	*Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y*	document member of the same patent family
document referring to an oral disclosure, use, exhibition or other means	*P*	
document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
11 JUNE 1999	19 JUL 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks 6000 PCT Washington, D.C. 20231 Facsimile No (703) 305-3230	Authorized officer AHMAD MATAR James R. Matthews Telephone No. (703) 305-3800